

DATA PROTECTION & PRIVACY POLICY

Updated for UK data protection law as in force in September 2026

Policy No.	11	Version	2.0
Policy Owner	Scottish Touch Board / Data Protection Lead	Approved by	Scottish Touch Board
Approval date	06/09/2026	Effective date	01/09/2026
Next review	01/09/2028	Contact	ceo@touch.scot
Status	Board-ready draft	Supersedes	STA Data Protection Policy v1.0

Purpose: This policy explains how Scottish Touch collects, uses, stores, shares and protects personal information and how individuals can exercise their data protection rights. It applies to Board members, staff, volunteers, coaches, officials, players, parents/guardians and anyone handling personal information on behalf of Scottish Touch.

1. Purpose and scope

Scottish Touch needs to process personal information in order to govern, administer and develop the sport of Touch in Scotland. This includes information relating to membership, competitions, representative programmes, the Youth Academy, coaching, officiating, volunteering, safeguarding, welfare, medical needs, communications, events, finance and marketing.

This policy applies to personal information in any format, including information held electronically, on paper, in photographs or video, and within approved platforms and communication systems used by Scottish Touch.

2. Current legal framework

Scottish Touch will comply with applicable UK data protection and privacy law, including:

- the UK General Data Protection Regulation (UK GDPR);
- the Data Protection Act 2018 (DPA 2018);
- the Data (Use and Access) Act 2025 (DUAA), which amends but does not replace the UK GDPR, the DPA 2018 and parts of the Privacy and Electronic Communications Regulations; and
- the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), where relevant to electronic marketing, cookies and similar technologies.

Where Scottish Touch provides or controls an online service likely to be accessed by children, it will also take account of the Information Commissioner's Age Appropriate Design Code (Children's Code) and the specific duties applying to children's personal information.

3. Roles and accountability

Scottish Touch is the data controller for personal information where it determines why and how that information is processed. In some circumstances another organisation may be an independent or joint controller, or a service provider may act as a processor on Scottish Touch's behalf.

The Scottish Touch Board has overall responsibility for data protection governance. A named Data Protection Lead will coordinate compliance, maintain relevant records, support responses to rights requests and complaints, and advise the Board. Scottish Touch will not use the title "Data Protection Officer" unless it is required to appoint a statutory DPO under applicable law or chooses to do so with the associated legal status and independence.

4. Data protection principles

Scottish Touch will process personal information in accordance with the UK GDPR principles. Personal information will be:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes and not used incompatibly with those purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept in identifiable form for no longer than necessary;
- kept secure using appropriate technical and organisational measures; and
- handled in a way that allows Scottish Touch to demonstrate compliance (accountability).

5. What information Scottish Touch may process

- identity and contact details, including names, dates of birth, addresses, email addresses and telephone numbers;
- membership, club, team, competition, selection and playing information;
- coaching, refereeing, volunteering, qualification, accreditation and training information;
- parent/guardian and emergency contact information for children and young people;
- attendance, travel, accommodation and event logistics information;
- photographs, video, media and communications preferences;
- financial and payment information where required;
- complaints, disciplinary, safeguarding, welfare and incident information; and
- health, medical, disability or other special category information where necessary to support safe participation or meet legal and safeguarding responsibilities.

6. Lawful bases

Scottish Touch will identify and document an appropriate lawful basis before processing personal information. Depending on the purpose, this may include:

- contract - where processing is necessary to provide membership, event or programme services requested by an individual;
- legal obligation - where processing is necessary to comply with a legal duty;
- legitimate interests - where Scottish Touch or a third party has a legitimate purpose and the processing is necessary and balanced against the individual's rights and interests;
- consent - where a genuine choice is appropriate and consent can be freely given, specific, informed and withdrawn; or
- vital interests - in limited circumstances involving protection of life or serious welfare needs.

Consent will not be treated as the default lawful basis merely because a form is signed. Where consent is relied upon, Scottish Touch will keep an appropriate record and make withdrawal as easy as giving consent.

7. Special category and criminal offence information

Special category information includes information about racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic or biometric information used for identification, health, sex life and sexual orientation. Criminal offence information is subject to separate legal safeguards.

Where Scottish Touch processes special category information it will identify both an Article 6 lawful basis and an applicable Article 9 condition, together with any additional condition required by the DPA 2018. Where required, Scottish Touch will maintain an Appropriate Policy Document. Criminal offence information will only be processed where the law permits and appropriate safeguards are in place.

8. Children and young people

Scottish Touch recognises that children merit particular protection in relation to their personal information. Information relating to Youth Academy and other under-18 participants will be handled with particular care.

- Privacy information will be clear, age-appropriate and understandable.
- Only information reasonably necessary for participation, safeguarding, welfare, logistics and administration will be collected.
- Parent/guardian information and consent will be obtained where required or appropriate, while recognising that data protection rights belong to the child and capacity should be considered as the young person matures.
- Information about children will not be published or shared for marketing or media purposes without an appropriate lawful basis and the necessary media permissions.
- Where Scottish Touch provides an online service likely to be accessed by children, their needs and best interests will be considered in the design and use of that service.

9. Privacy information and transparency

Scottish Touch will provide appropriate privacy information when personal information is collected, or otherwise within the time required by law. Privacy notices will explain, as relevant, what information is collected, why it is used, the lawful basis, who it may be shared with, retention, international transfers, rights and how to complain.

10. Data collection and minimisation

Information will be collected only where there is a clear purpose. Forms, spreadsheets, shared drives and digital platforms should not collect or retain information simply because it may be useful in future. Where information is already held securely in an approved system, volunteers should avoid creating unnecessary duplicate copies.

11. Digital platforms and communications

Scottish Touch may use approved third-party services such as SportMember, WhatsApp, Instagram, email, cloud storage and other systems for administration, communication, logistics and marketing. Before adopting or materially changing a service, Scottish Touch should consider the provider's role, security, contractual terms, retention, access controls, international transfers and privacy implications.

- SportMember should normally be used for structured membership, attendance, scheduling and participant information where that functionality is available.
- WhatsApp and similar messaging tools should not be used as long-term repositories for medical, safeguarding or other sensitive information. Sensitive matters should be moved to an appropriate secure channel and recorded in the relevant official system where necessary.
- Access to official accounts and groups must be role-based and removed promptly when a person leaves the relevant role.
- Personal information must not be copied into personal devices, spreadsheets or messaging threads unless necessary and appropriately protected.

12. Data sharing and processors

Scottish Touch may share personal information with clubs, competition organisers, governing bodies, insurers, venue providers, travel providers, medical or safeguarding personnel, professional advisers, service providers, public authorities or others where there is a lawful and necessary reason to do so.

Where a supplier processes personal information on Scottish Touch's instructions, appropriate processor terms will be put in place as required by law. Scottish Touch will not sell personal information.

Information may be disclosed without consent where another lawful basis applies, including where disclosure is necessary to protect someone's vital interests, comply with law, manage safeguarding concerns, establish or defend legal claims, or cooperate with appropriate statutory authorities.

13. International transfers

Where Scottish Touch makes a restricted transfer of personal information outside the UK, it will ensure that an appropriate transfer mechanism is available, such as UK adequacy regulations or approved safeguards. Where required, Scottish Touch will carry out the applicable transfer risk assessment/data protection test and implement supplementary measures.

14. Data security

Scottish Touch will apply security measures appropriate to the nature and risk of the information processed. These may include:

- role-based access and least-privilege permissions;
- strong passwords and multi-factor authentication where available;
- secure storage and controlled sharing of files;
- device security, updates and appropriate encryption;
- care when sending email and checking recipients before sending;
- secure disposal and deletion of paper and electronic records;
- training and guidance for people who handle personal information; and
- regular review of access when roles change.

15. Retention and disposal

Personal information will be kept only for as long as required for the purpose for which it was collected, taking account of legal, safeguarding, insurance, financial, sporting and operational requirements. Scottish Touch will maintain or develop an appropriate retention schedule. Records that are no longer required will be securely destroyed or anonymised.

16. Individual rights

Subject to the conditions and exemptions in data protection law, individuals may have rights to:

- be informed about processing;
- access their personal information;
- have inaccurate information rectified;
- have information erased in certain circumstances;
- restrict processing in certain circumstances;
- receive and transfer certain information (data portability);
- object to certain processing, including direct marketing; and

- receive safeguards in relation to solely automated decisions that have legal or similarly significant effects.

Scottish Touch will verify identity where reasonably necessary and will respond to rights requests within the applicable statutory timeframe. The Data (Use and Access) Act 2025 clarifies aspects of the right of access, including the approach to reasonable and proportionate searches for information.

17. Data protection complaints

Scottish Touch will provide a clear and accessible way for individuals to complain about how their personal information has been handled. In accordance with the Data (Use and Access) Act 2025, Scottish Touch will:

- take reasonable steps to facilitate data protection complaints, including an electronic route for making a complaint;
- acknowledge receipt of a data protection complaint within 30 days;
- without undue delay, take appropriate steps to investigate and respond, keeping the complainant informed where appropriate; and
- without undue delay, tell the complainant the outcome.

Individuals also have the right to raise concerns with the Information Commissioner's Office (ICO).

18. Personal data breaches

A personal data breach includes accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information. Anyone acting for Scottish Touch who becomes aware of a suspected breach must report it immediately to the Data Protection Lead.

- Scottish Touch will take prompt steps to contain and investigate the breach and assess risk to individuals.
- All personal data breaches will be documented, whether or not they are reportable to the ICO.
- Where a breach is likely to result in a risk to individuals' rights and freedoms, Scottish Touch will notify the ICO without undue delay and, where feasible, within 72 hours of becoming aware of it.
- Where a breach is likely to result in a high risk to individuals, affected individuals will be informed without undue delay where required by law.

19. Data protection impact assessments and privacy by design

Scottish Touch will consider privacy and data protection at the start of new projects, systems, programmes and significant changes. A Data Protection Impact Assessment (DPIA) will be completed where processing is likely to result in a high risk to individuals, and may also be used as good practice for significant new technology, large-scale sensitive data, systematic monitoring or new uses of children's information.

20. Direct marketing and media communications

Where Scottish Touch sends direct marketing by electronic means, it will comply with the UK GDPR, the DPA 2018, PECR and the changes made by the Data (Use and Access) Act 2025. Individuals will be given

appropriate information and a simple way to opt out where required. Marketing preferences will be respected and suppression records may be retained where necessary to ensure that an opt-out continues to be honoured.

21. Training and responsibilities

- Board members, staff and volunteers who handle personal information must follow this policy and relevant procedures.
- Appropriate data protection training or guidance will be provided for roles with regular or sensitive data handling responsibilities.
- Personal information must only be accessed or used for legitimate Scottish Touch purposes and within the scope of the person's role.
- Suspected misuse, loss or unauthorised disclosure must be reported promptly.

22. Monitoring and review

The Board will periodically review Scottish Touch's data protection arrangements, including significant risks, incidents, complaints, rights requests, key service providers, retention arrangements and training. This policy will be reviewed at least every two years, and earlier where there is a significant change in law, ICO guidance, systems or Scottish Touch operations.

23. Contact

Data Protection Lead: [insert name / role]

Email: [insert data protection email]

Appendix A - Key definitions

Term	Meaning
Personal information / personal data	Information relating to an identified or identifiable living person.
Processing	Any operation performed on personal information, including collection, recording, organisation, storage, alteration, retrieval, consultation, use, sharing, restriction, deletion or destruction.
Data controller	The person or organisation that determines the purposes and means of processing personal information.
Data processor	A person or organisation that processes personal information on behalf of a controller.
Data subject	The identified or identifiable living person to whom personal information relates.
Special category information	Personal information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; genetic data; biometric data used for

	identification; health data; and information about sex life or sexual orientation.
Personal data breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information.
DPIA	A Data Protection Impact Assessment used to identify and reduce privacy risks, required for processing likely to result in high risk.
ICO	The Information Commissioner's Office, the UK regulator for data protection and information rights.

Appendix B - Legislative and regulatory references

- UK General Data Protection Regulation (UK GDPR).
- Data Protection Act 2018.
- Data (Use and Access) Act 2025.
- Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), as amended.
- Information Commissioner's Office guidance, including current guidance on data protection complaints, personal data breaches, international transfers and children's information.
- Age Appropriate Design Code (Children's Code), where applicable.